SYNOPSIS OF THE THESIS

Entitled

SECURITY ENHANCEMENT OF IOT NETWORK SYSTEM USING OPNET FOR OPTIMIZED DEVICES

Submitted to

SWAMI RAMANAND TEERTH MARATHWADA UNIVERSITY

NANDED (M.S.)

In partial fulfillment for the award of the degree of

DOCTOR OF PHILOSOPHY

In the subject of

COMPUTER SCIENCE

Under the faculty of Computational Sciences

Submitted By

M.ANJANEYULU

Research Scholar

School of Computational Sciences

Sri Ramanand Teerth Marathwada University

Nanded-(M.S).

Under the Guidance of

Dr.S.B.THORAT

Research Guide

Director

Shri Sharda Bhavan Education Society's, ITM College,

VIP Road, Nanded.(M.S.)

INDEX

S.No.	Content	Page No.
1	Abstract of proposed work plan/ problem:	3
2	Introduction	3
3	Review of Literature and Development in the subject (Previous work done in the relevant area):	9
4	Objectives of Research/ Proposed Hypothesis:	14
5	Methodology to be adopted:	14
6	Importance of study/ Society application:	18
7	Year-wise Plan of work and targets to be achieved	19
8	References:	20

SECURITY ENHANCEMENT OF IOT NETWORK SYSTEM USING OPNET FOR OPTIMIZED DEVICES

Abstract

Known as the Internet of Things (IoT), it is an emerging worldview characterized by heterogeneous advancements that are made possible by savvy omnipresent articles that are flawlessly associated with the Internet. The Internet of Things (IoT) is a term that refers to a growing body of knowledge about the Internet. It is recommended that Low Power and Lossy Networks (LLN) and Fog Security Service (Nadeem Abbas et al., 2019) be used to offer security for new services in a variety of application areas, such as smart cities, smart health, and smart communities, as part of the proposed study. The low-latency network (LLN) is a kind of network in which the associated devices are severely resource restricted, and which is characterized by high loss rates, low data rates, and instability in the communication channels. Aside from that, Internet of Things devices create a significant volume of private and security-sensitive data. Different cryptographic-based systems are available that are capable of adapting to security assaults; however, they are not suited for IoT due to the large amount of resources they need. The proposed study will examine how well the Fog Security Service (FSS) performs for Internet of Things (IoT) devices while using two well-known cryptographic schemes: identity-based encryption and identity-based signing, as well as other techniques. The suggested design, which is a single network topology with varying traffic loads, will be modelled using the OPNET simulator.

Keywords: Internet of Things, LLN, OPNET, Security, Network.

1. Introduction

In its most basic definition, the Internet of Things (IoT) is a global network of individually accessible networked objects that are capable of detecting, communicating, and processing, as well as providing services and doing data analysis. Doorbells, sensors, Digital Video Recorders (DVRs), light bulbs, electric switches, and home assistant devices are examples of Internet of Things (IoT) products. At the core of the Internet of Things (IoT) network are Near-Field Communications (NFC) and Wireless Sensor and Actuator Networks (WSAN), which are linked by Radio-Frequency Identification (RFID) technology (RFID). In recent years, as a consequence of the convergence of the Internet and sensor networks, machine-to-machine (M2M) communication has evolved on the Internet, enabling a huge number of autonomous and self-organized devices to interact

with one another. This 20-year-old concept has moved from RFID systems to the present IoT research boom, which is resulting in more deployments of this 20-year-old concept. Microcontrollers are small electronic devices that are about the size of a credit card and are utilized as embedded sensors, actuators, and other devices to conduct distant and occasionally autonomous operations. They are substantially less resource-efficient than today's desktop PCs, despite the fact that some of these devices are more sophisticated than the computers that enabled men to land on the moon. As previously stated, many of today's cyber security solutions are designed to work with these desktop-type computers, which continue to constitute the vast bulk of the Internet's user base. These gadgets, on the other hand, will no longer be the primary targets. There has already been an alarming increase in the proliferation of the Internet of Things (IoT), which has resulted in an enormous increase in the number of attack surfaces that are vulnerable. Without adequate Internet of Things security that is tailored to these little devices, threats will abound in many sectors of our life, including healthcare, automobiles, and vital infrastructure.

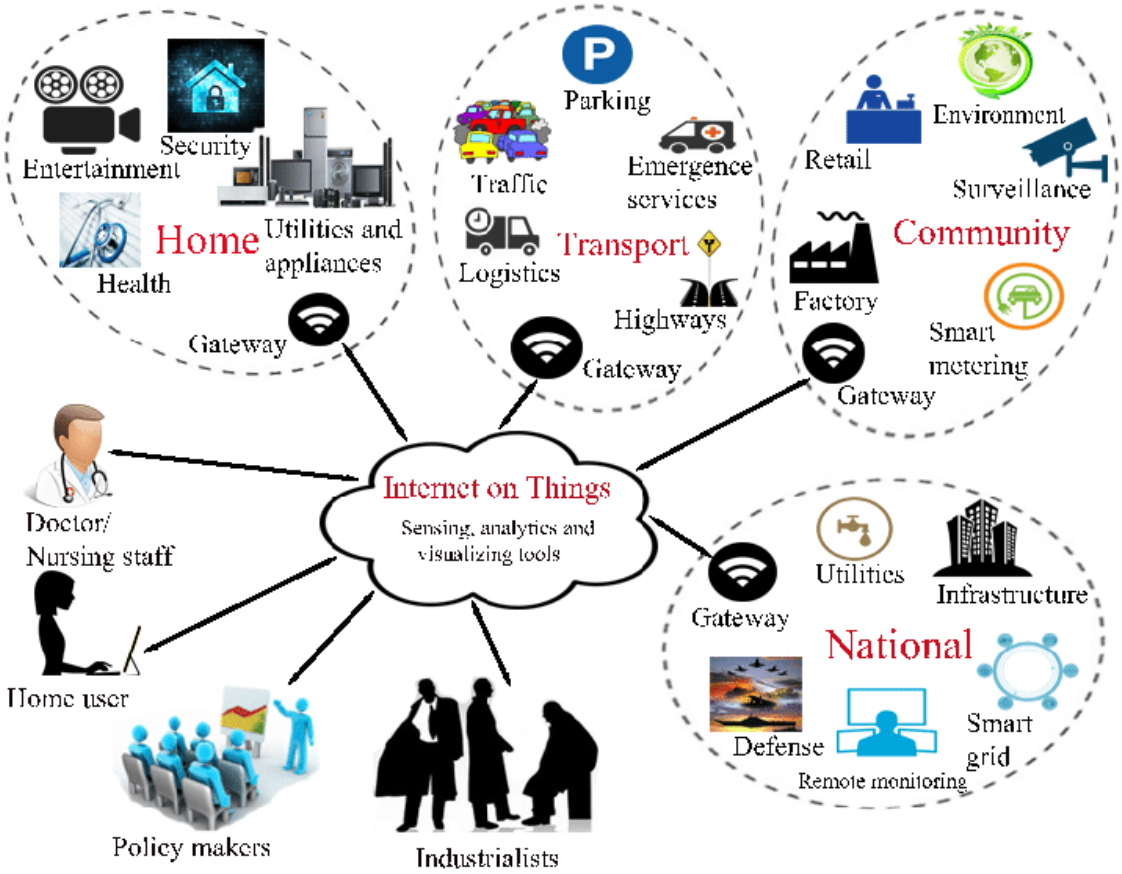

Fig No.1 Internet of Things Utility

1.1 Enabling Technology

The Internet of Things (IoT) is a built-in device collection for Internet and manual sense communication that is connected to the Internet. As a consequence, we shall travel over three of the most essential Internet of Things technologies that are included in this part. Three technologies are being examined: the Internet Protocol Version 6 (IPv6), radio frequency identification (RFID), and wireless sensor networks (WSN). This is not to say that it is not a comprehensive list of IoT technology, but it does not include intelligent sensitivity, NFC, cloud computing, global positioning system (GPS), service architecture (SOA), geographical information system (GIS), and mobile cellular devices, among other things. It has been summarized.

- **Internet Protocol Version 6**

The Internet protocol version 6 (IPv6) was designed as a result of the expiration of the currently available IP addresses under the IPv4 scheme. The IPv6 protocol gives 2128 IP addresses, which is a significant increase above the 232 IP addresses available under the IPv4 system. This is crucial for IoT since the number of smart devices and sensors planned to be connected to the Internet will rapidly deplete the IPv4 protocol's remaining address space.

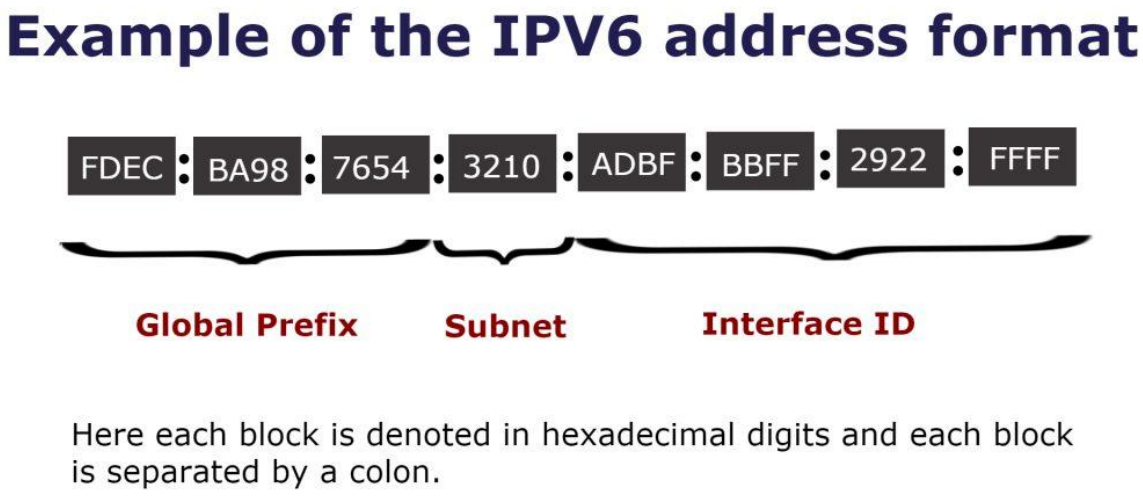
Example of the IPV6 address format
FDEC : BA98 : 7654 : 3210 : ADBF : BBFF : 2922 : FFFF
Global Prefix
Subnet
Interface ID
Here each block is denoted in hexadecimal digits and each block is separated by a colon.

Fig No-2 IPV 6 example

- **Radio Frequency Identification**

One of the most essential technologies in the Internet of Things is radio frequency identification (RFID), which is becoming more widespread (RFID). When it was employed to identify friendly aircraft during World War II, it was still a relatively new technology in the commercial and civilian sectors. It was also not particularly portable or energy efficient at the time. RFID tags and RFID readers are the two primary components of RFID technology. RFID tags and RFID readers are interchangeable. RFID tags and RFID readers are interchangeable in their functionality. RFID tags may be linked to anything that we wish to monitor or gather data from, and RFID readers are devices that can detect and read the data contained in RFID tags. RFID tags are becoming more popular. RFID tags and RFID readers are two separate types of devices that communicate with one another. RFID technology may also be used to wirelessly extract information from tagged things by transmitting radio waves.

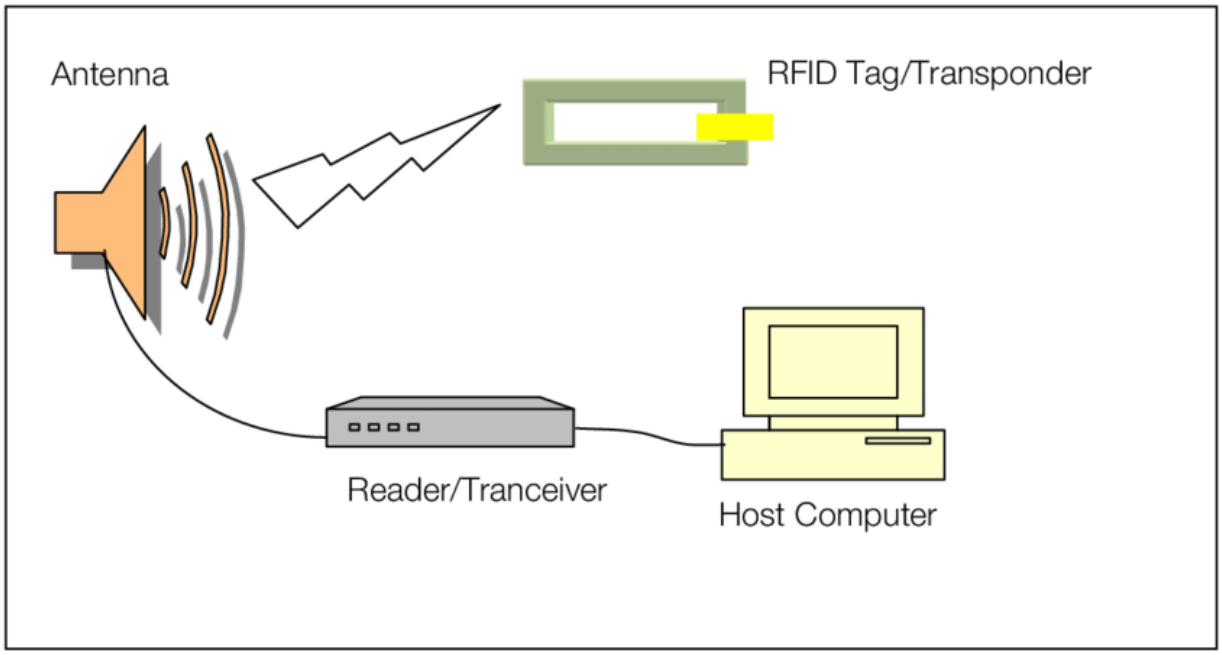

Fig No. 3 Radio Frequency Identifier

- **Wireless Sensor Networks (WSNs**

It is common for wireless sensor networks (WSNs) to be composed of a collection of sensor devices distributed throughout a geographic region that collect and transmit data to a central receiving unit, which then sends that information to a data warehouse for further processing and analysis. Therefore, receiver devices are often more powerful than sensor devices since they

must analyse all incoming data, do some processing before sending the data to a backend system, which requires more computing power.

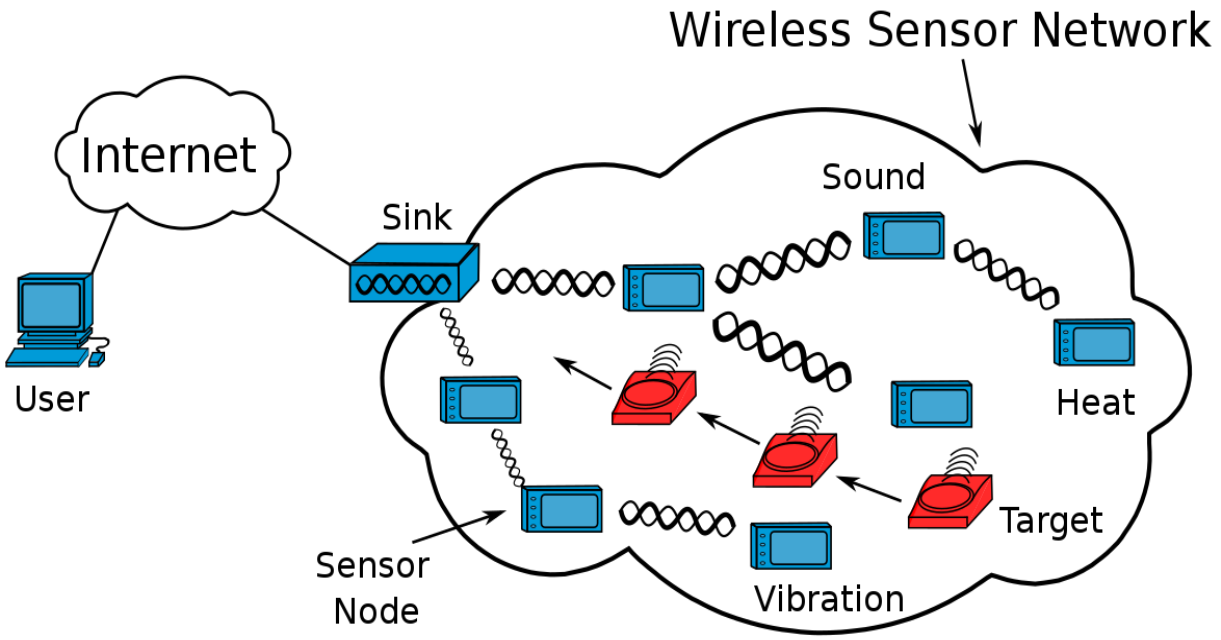

Fig No-4 Wireless Sensor Network

1.2 Applications of IoT as per current scenario:

- **Business and Industrial applications**

The Industrial Internet of Things (IIoT), which includes industrial and manufacturing enterprises, is a significant industry that has already benefited from the Internet of Things (IoT) technologies. The Fourth Industrial Revolution, which includes the Internet of Things, is referred to as "Industrial 4.0," which is an abbreviation for the Internet of the Fourth Industrial Revolution and things. The Internet of Things (IoT) makes use of a massive quantity of data collected from sensors and other devices in order to enhance operations while avoiding cost savings and mishaps from occurring. To boost the efficiency of delivery procedures, Amazon, for example, employs an autonomous robot to monitor retention and collect client orders. Also anticipated to be better understanding of defects or delays that can be more efficiently transferred information on production lines and decreasing information on production lines, as well as to minimise inventory costs and unload them in other parts of Paris, thanks to the Internet. A large number of networked devices that communicate data on a continuous basis throughout the manufacturing and production lifecycles make it feasible for this to happen.

- **Smart Consumer & Homes**

The last scenario described is directly applicable to the regular customer. As a result of the massive quantity of data that is generated by the Internet of Things (IoT), businesses may tailor their client interactions. Early adopters' houses are likely to have equipment that are linked to the internet. Customers who are technologically knowledgeable and who desire the newest technology in their life and at home may easily sell smart security systems, smart gadgets, voice assistants such as Alexa, and other related products to them. However, industry observers claim that, despite the fact that this frenzy seems to be receding, an increasing number of firms are racing to build Internet-connected gadgets in a range of sectors. Unfortunately, engineers who add internet capabilities to refrigerators are not required to be security specialists, and ordinary smart products are at danger of being hacked as a result. Even for firms that are concerned about security, the deployment of an always-on, Internet-connected gadget presents significant commercial hurdles.

- **Healthcare**

  Another crucial factor to take into consideration is health-care coverage. It is the goal of the Internet of Things (IoT) to lower healthcare expenses by allowing consumers to communicate digital information to healthcare experts in a more timely and effective manner than previously possible. Wearable gadgets that are linked to the Internet enable physicians and caregivers to monitor and care for patients without the need to physically visit a hospital or a clinic location. Consequently, the health-care system will be less crowded, alleviating issues such as a shortage of beds and overwhelmed physicians and nurses. Unfortunately, the fact is that this may result in the violation of one's personal privacy, which is unacceptable. Given the fact that these carriers are incredible for individuals and retain personal information, there is a big problem with severe confidentiality difficulties with IoT integration on heath care systems, which is a problem. New technologies are also being employed to aid in the treatment of diseases such as diabetes and Parkinson's disease, among others. However, when wireless connectivity is included, the potential of personal data being compromised rises. You can track someone, for example, if you provide an ID that a device may detect as belonging to a certain individual, similar to the way the automobile industry follows people who use the Tire Pressure Monitoring System (TPMS) and have it fail.

1.3 Challenges in IoT Security

There were many use cases described in the preceding scenarios, each with its own set of security concerns and benefits associated with the addition of Internet connection to previously offline systems. In the wake of a comprehensive assessment of these events and relevant literature, ten major challenges were identified and prioritised based upon their impact on Internet of Things security:

- **Standardization**
- **Trust & Authentication**
- **Privacy**
- **Information Security**
- **Network Attacks**
- **Latency**
- **Wireless networks are used for communication**
- **Version control and software upgrades are two important aspects of business.**
- **Physical Attacks**
- **Size, Weight, and Power**

2. REVIEW OF LITERATURE

- **Wang et.al. (2019)**In the essay, the authors explore the handling of IoT security risks. Using both static and dynamic features of objects, the authors of this paper investigated machine-to-machine communication between two machines in their research. When a sensor is detected by Dynamic, it records the information on the label. Internet of Things refers to a network of machines that are linked to the Internet, and the integration of heterogeneous networks is a recent trend in network development, according to the Internet Society. It is responsible for a broad variety of algorithms, including load balancing, power management, congestion control, transition management, and others. It is also responsible for network resource management. The key subjects discussed in this research are machine-to-machine data transfer, sensor technologies, and security.
- **Wang et.al. (2019)**The authors discussed IoT security management in their paper. Using the static and dynamic features of objects, the authors of this work have

studied machine-to-machine communication between two machines. On the other hand, Dynamic recognizes the sensor and saves the information in the label. The Internet of Things is a network of machines that are linked to the internet, and heterogeneous network integration is the current trend in network development, according to the Internet Society. Network resource management is responsible for a wide range of algorithms, including load balancing, power control, congestion control, control switch, and others. M2M transmission, sensor technology, and security are all topics that will be covered in depth in this research.

- **Suo et.al. (2018)**The writers have looked at the possibility of future uses in the sector. In this research, the authors recommend using an encryption technique, network security, and sensor information shielding to protect sensor information. Many earlier systems made use of the cloud for security-related operations such as key generation, certification, and authentication, among other things. Nevertheless, when there are a large number of IoT devices, these strategies become unfeasible, and a faster response time is necessary in order to improve service quality and overall safety.
- **Chen et. al.(2018)**The authors have addressed IBE, or identity-based encryption, which is a kind of encryption that may be used by both men and women. We make use of three levels of abstraction: middleware, perceptron layer, and applied middleware. It was also possible to use RFID (radio frequency identification). This is the system that allows you to recognize individuals without having to physically touch them. In this article, the authors discuss the elliptic curve cryptosystem as well as identity-based encryption techniques. Both of them make use of public key cryptography to protect their information. In this article, the authors provide an overview of fog applications as well as the security issues that might arise as a result of using them. When it comes to fog computing, the scientists were particularly interested in man-in-the-middle attacks, in which fog devices may be compromised or swapped with bogus ones.
- **Poslad et.al. (2017)**The authors have researched Identity-Based Encryption (IBE) and believe that males will be more inclined than women to employ it.

Middleware, the perceptron layer, and the application middleware are the three processing layers that we use. There was also the usage of a radio frequency identification (RFID) technology. Anyone may be identified by this procedure, which does not need the actual contact with the individual. It was the authors' intention in this paper to cover topics of elliptic curve cryptography and identity-based encryption. These two are encrypting their communications using public key cryptography. The writers of this white paper have offered an outline of fog applications and the security challenges that have arisen as a result of them. Man-in-the-middle attacks, in which fog computing devices may be hacked or substituted with counterfeit items, were of particular interest to the authors in the context of fog computing, according to their research.

- **Razzaq et.al. (2017)**The writers discussed how many people use the Internet and how many nations have access to the Internet, as well as how many people use the Internet. Not only will the surroundings in which you live change, but so will all of the acts that you do in your daily life as well. When there is an Internet of Things, the safety device is breached in 70 percent of the cases that were investigated, according to the researchers. This book also covers a wide range of themes, including industry, medical gadgets, smart homes, and a variety of other ideas. According to the study's author, the only way to avoid assaults from genuine devices is to use a secure network infrastructure.
- **Raja et.al. (2016)**In the author's opinion, the introduction of a new security paradigm is not far off. When it comes to the functioning of a security system, emotions are quite significant. Wireless security has been more popular in recent years, owing to the simplicity with which it can be installed and operated. The installation of a home security system is the primary emphasis. The most significant disadvantage is that it is both costly and difficult to deploy. The writers of this article discuss the RASPBERRY PI and, among other things, demonstrate how to write code that allows a device to run the Raspbion operating system by executing a Python script on it. It is equipped with a variety of features, including an email and SMS system as well as a motion detection system.

- **Tahir et.al. (2016**) The author has explained how to interact with people via the use of the Internet and a mobile phone with the audience. In order to do this, you must create a connection within the range of Wi-Fi, Bluetooth, and other wireless devices. Architecture of fog software highlights the author's improvement of the numerous technological components that the author used to implement the paradigm fog software at a high degree of abstraction. Advanced advanced programming for online applications is made possible by the mobile fog idea, which is a sensible and extended terrain spatial dispersed internet application. There are several security studies and secret issues about shaky internet connectivity that have been documented in the literature.
- **Barcena et.al. (2016)**The writers looked at a number of different security applications, including consumer electronics, physical access, and Ethernet. When constructing networks, what kind of home appliances are employed and how do they function? During an assault, it is feasible to get physical access. They also utilise malware or malicious software to connect with smart homes, smart grids, and home automation systems, as well as other electronic devices.
- **Kumar et.al. (2015)**The author of this article demonstrates how people may access to the Internet at any time and from any location by using touch devices and wireless networks. In the case of the Internet of Things, for example, many other scientists are trying to design applications that may be utilised in conjunction with various architectures. MAC, on the other hand, is used in a unique manner (media access control). Additionally, there is still a great deal of work to be done since the Internet of Things security procedure will not be completed.
- **Suchitra and Vandana(2015)**This problem has already been considered in terms of diary potential and concerns associated to the Internet, and past academics have verified that this is a topic that is worth further investigation. The author of this page discusses how the service (DDoS) is utilized, as well as how DDoS assaults are carried out without the use of any DDoS. They increase the security of Internet of Things devices in order to improve the security of the Internet of Things device, by creating a fog that diffuses input from the Internet of Things

device, and this is a promising path in my view. According to this technique, the cloud is used to keep and update the list of certificates that the certification authority supports, and it is also used to update and make certificates available for usage on a regular basis via the cloud, among other things. On the other hand, most businesses may be reluctant to offer a security certificate for a cloud since they do not have confidence in cloud service providers.

- **Kai et.al. (2014)**Using the Internet of Things as a framework for discussion, the writers addressed smart health. Consider how drastically different the situation is when it comes to security and privacy in the healthcare industry: One-fifth of the country's workforce is employed by the information and communications technology (ICT) sector. In the study's authors' words, the authors were testing the security of the medical system in question. According to the new Internet of Things health plan, this is correct. It is necessary to migrate processing and storage resources to the cloud in order to accomplish time-consuming authentication activities with the least amount of delay and power consumption. An authentication and user management architecture for SaaS cloud services has been built, according to the findings of the research. This design makes advantage of the security properties of Jason Web Tokens (JWTstateless) for client authentication as well as session management.
- **Zhao et.al. (2014)**The author investigated the Internet of Things (IoT), current applications, and its potential uses in the future. The authors of the research have made recommendations on methods to mitigate the hazards associated with the Internet of Things. Making use of a policy-based fog resource security management technique, the authors demonstrate how to undertake policy analysis and integrate it with the fog paradigm, as well as other aspects of resource security management. This technique, on the other hand, does not take into consideration the inheritance and propagation of rights within an ecosystem.

3. OBJECTIVE OF THE RESEARCH

- To perform simulations based analysis to examine the performance and to verify the effectiveness and efficiency of the proposed models.
- To incorporate Hybrid approach using Identity based Encryption and Identity based Signature for better performance accuracy.
- To critically evaluate the impacts of Hybrid approach and LNN in performance betterment of the model.

4. METHODOLOGY TO BE ADOPTED

This proposed work would adopt following methods in order to meet the objective:

- **Low Power and Lossy Networks (LLN)**

  Significant losses in low-power networks are characterized in the following ways: The majority of the time, the power, memory, and processing resources are limited, and the device is configured as a built-in device via a variety of different purposes. Compounds such as IEEE 802.15.4 and Wi-Fi Snowless are examples of this. Industrial monitoring is not the only application for this technology. Building automation includes heating, ventilation, and air conditioning (including HVAC, lighting, access control, and fire), linked homes, health monitoring, environmental monitoring, touch networks, power management, asset and cooling tracing, and many other applications. Some LLN-related applications. So NEADERPOWER and LETTYNETWORKS often exhibit some of the average stability, but also frequently exhibit not only a few simple trusts, but also a few simple trustworthy volatility of delivery, as a consequence of this. Routing and doing measurements along the same edge, such as estimating the anticipated number of transmissions, are two examples of edge computing. Typical low-power networks that experience large losses include the following: In most situations, the network is powered by a small amount of electricity and has limited memory and computational capabilities, which are configured as the built-in device via a variety of tasks. Compounds such as IEEE 802.15.4 and Wi-Fi Snowless are examples of this. Industrial monitoring is not the only application for this technology. Building automation includes heating, ventilation, and air conditioning (including HVAC, lighting, access control, and fire), linked homes,

health monitoring, environmental monitoring, touch networks, power management, asset and cooling tracing, and many other applications. Some LLN-related applications. So NEADERPOWER and LETTYNETWORKS often exhibit some of the average stability, but also frequently exhibit not only a few simple trust, but also a few simple trustworthy volatility of delivery, as a consequence of this. Routing and doing measurements along the same edge, such as estimating the anticipated number of transmissions, are two examples of edge computing.

- **Fog Security Services (FSS)**

  The identity-based encryption and identity-based signature techniques are two cryptographic technologies included in this grouping.

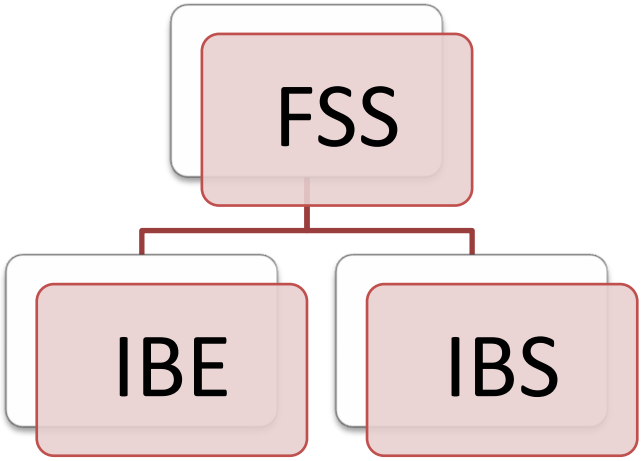

Fig No-5 Hybrid Method

- **Identity-based encryption**

  Using a well-known unique identification (for example, an e-mail address) and producing a user's public key, as well as constructing a closed key generation for a trustworthy server, is an example of PublicKe encryption. Key that is available to the public. If you choose to use this approach, you will not be required to deploy an open key prior to transmitting encrypted data. The sender must employ a unique recipient identification number to complete this process, which will result in the creation of a public key and the encryption of the data. A private key associated with the message may be generated using a prestigious server by the ThreeParty – PowerKey Generator - The receiver using a prestigious server (PKG). PKG first releases the default public key, and then stores the default closed key that corresponds to the encryption

technique being used by the package (called the default key). As long as you use the primary open key with well-known identifying values, everyone can generate an open key that can be used by everyone else (for example, an email address) to produce an open key that can be used in a variety of situations (that is, email address). It is necessary to communicate with the PKG to build the suitable closed keys using the primary private keys in order to get the ID owner generated by the public key in order to obtain the proper closed key. It is then sent to the ID that was used to create the public key.

- **Single Network Topology**

This approach may be considered to be a combination of the four algorithms outlined below, with the identity-based signature method being the culmination of these algorithms. custom. In response to secure input, the master executes this procedure in order to create public schema choices and master secrets for the schema under consideration. A master object exposes parameters while keeping the master object itself concealed from the rest of the object hierarchy. Extraction It produces a private key du of ID u, given ID u, master secret, and parameters from the supplied ID u and parameters. A secure communication channel is used by the master entity in order to produce private keys for all entities participating in the plan and to send those private keys to their respective owners.

- **Analysis with Multiple Traffic Loads**

In the proposed methodology analysis using different loads for each not is to be done in order to check the performance and to make the model optimized.

- **Tools and Techniques used.**
- **OPNET**
    - The OPNET Network Simulator is a programme that may be used to model the behavior and performance of any network. When compared to other simulators, the key distinction between OPNET Network Simulator and others is its power and variety. Software, models, and documentation are the three components of OPNET Modeler.
    - Simulation runs at the "packet-level" using OPNET, a high-level event-based network simulation tool.

- Originally designed to simulate fixed networks.
- OPNET has a large collection of realistic simulations of fixed network hardware and protocols that are commercially accessible.
- The options for wireless network simulations are likewise fairly broad nowadays.
- Accurate radio transmission pipeline stage for physical layer modelling (radio interface)
- The simulator has a lot of promise, but it usually lacks the most latest wireless technology.

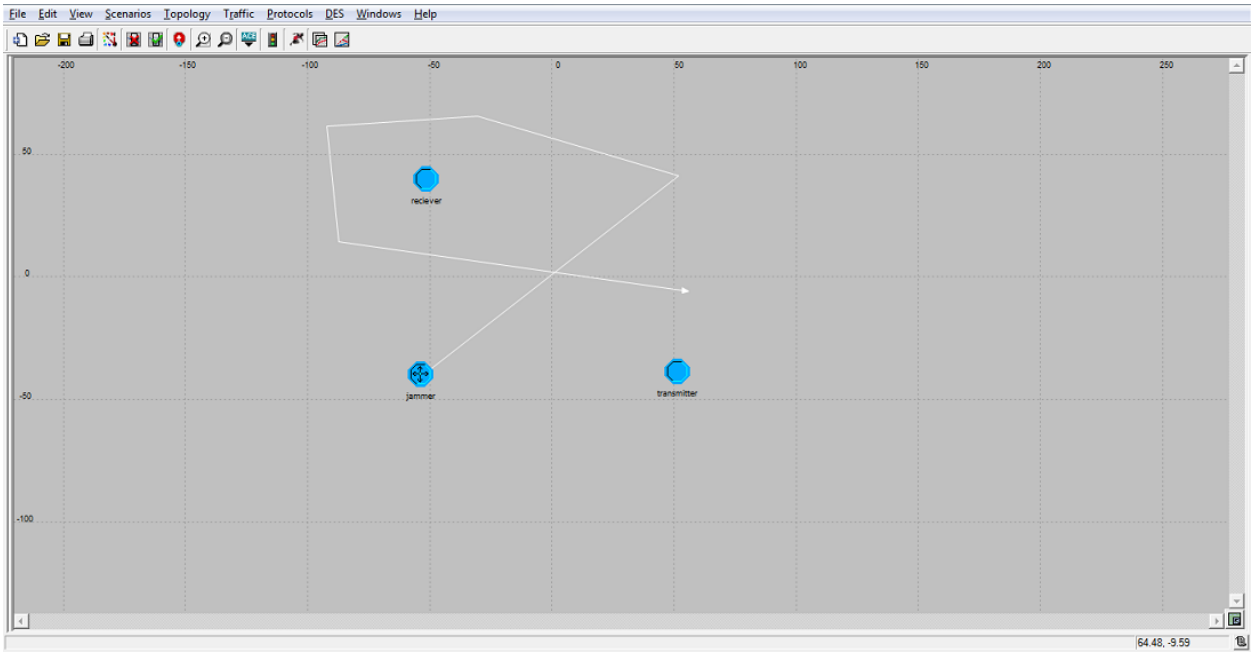

Fig No-6 OPNET Modeler overview

- **The OPNET simulator modeling is divided into three main domains:**
  - Network domain
  - Networks + sub-networks, network topologies, geographical coordinate mobility
  - Node domain
  - Nodes in a single network (e.g., routers, workstations, mobile devices)
  - Domain of the process
  - Inside network nodes, single modules and source code (e.g., data traffic source model, IP protocol)

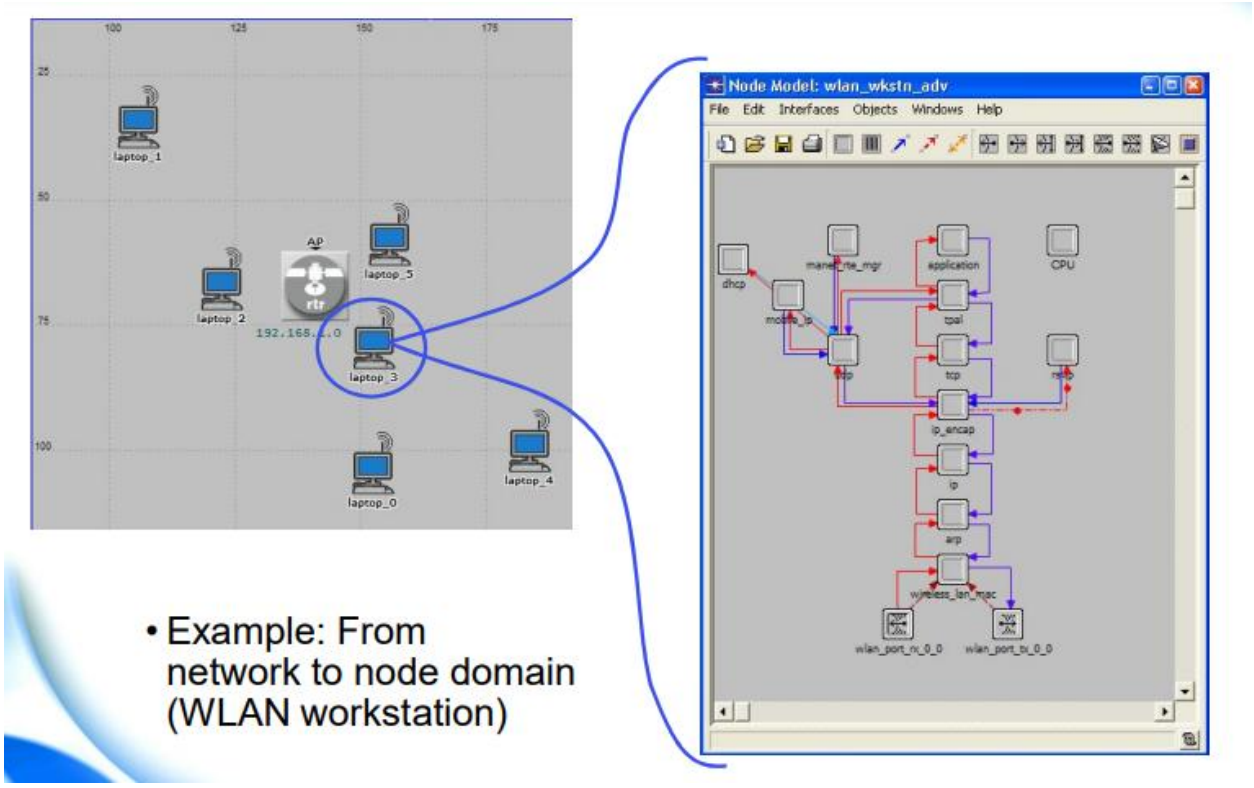

Fig No-7 OPNET Network Simulation

5. IMPORTANCEOF THE STUDY

Every second, the number of devices connected to the Internet grows in tandem with the advancement of the whole globe and the advancement of all technological advancements. The Internet of Things (IoT) provides a solution that eliminates the need for human labor. Nonetheless, there are certain limitations, such as those related to security and secrecy. Because of the increasing number of devices connected to a network, the operating system is on the operating system list. It will become tougher. All of these new immigrants are becoming more difficult to handle at the current pace of implementation of existing procedures. Customers become more crucial as a consequence of their growing anxiety about personal data breaches, information theft, and a variety of other difficulties. A system problem may occur due to an attack on the Internet, as we all know. An assault on the Internet can cause a typical system to fail. There are several researchers who concentrate on a variety of topics such as how to collect data, how to expand the number of health-care systems, and how to develop intelligent agriculture systems. As part of your personal and professional life, you will also employ Internet of Things technology to offer access to conference information that has never before been

available to you. Maintaining public safety as a consequence becomes more critical. A wide range of modern technologies and gadgets are available on the Internet, and security concerns around technology are significant. Consequently, to ensure that IoT settings remain safe, the security risks that arise in this approach are inherited by this technology, and as a consequence, each significant technology integrated into the kit must be secure in both cases. The integration of heterogeneous technologies, particularly heterogeneous technologies in and of itself, may lead to the introduction of a new vulnerability that does not exist on a standalone system as a consequence of this integration.

6. PROPOSED WORK PLAN

ANALYSIS DESIGN AND IMPLEMENTATION ENHANCEMENT OF IOT SECURITY USING OPNET FOR OPTIMIZED DEVICES						
Sl.No.	Project Module	Weightage	Completion %	Month Wise Planned %		
		100%		Year-1	Year-2	Year-3
1	Literature Survey	5%	10%			
2	Research Gap	5%	100%			
3	Research Objective	5%	100%			
4	Study for Methodology	5%	5%			
5	Tools and Techniques	3%	5%			
6	Data Collection	8%	0%	100%		
7	Data Processing	8%	0%			
8	Model Building	8%	0%			
9	Model Configuration	8%	0%			
10	Model Deployment	8%	0%			
11	Chapter 1	4%	0%			
12	Chapter 2	4%	0%		100%	
13	chapter 3	4%	0%			
14	chapter 4	4%	0%			
15	chapter 5	4%	0%			
16	chapter 6	4%	0%			
17	chapter 7	4%	0%			
18	chapter 8	4%	0%			
19	Poofread	5%	0%			100%

7. CONCLUSION AND FUTURE SCOPE

An optimized way of security of the IoT enabled device is expected as an outcome of the proposed work. The proposed work also compares the alternative methods with the proposed method to check for the performance. The characteristics of the LNN will help to make future research to be more effective and energy efficient. The proposed model would suggest the best alternative options. This approach will help to reduces service latency and will improve the Quality of Service (QoS), and provides a superior experience to end-users. In the future the iterative approach can be adopted with different methods.

REFERENCES:

[1] Kun Wang JianmingBao and Meng Wu Weifeng Lu "Research on Security Management for Internet of Things" 201O International Conference on Computer Application and System Modeling Vol-I5 pg- 133 to 137.

[2] SarfrazAlam, Mohammad M. R. Chowdhury and Josef Noll "Interoperability of Security-Enabled IoT" Wireless Commun (2011) vol-61:567–586.

[3] HuiSuo, Jiafu Wan, CaifengZou and Jianqi Liu "Security in the Internet of Things: A Review" 2012 International Conference on Computer Science and Electronics Engineering pg-648 to 651.

[4] Wang Chen "AN IBE-BASED SECURITY SCHEME ON INTERNET OF THING 2012 Proceedings of IEEE CCIS pg- 1046 to 1049.

[5] Stefan Poslad, Mohamed Hamdi and HabtamuAbie" International Workshop on Adaptive Security & Privacy management for the Internet of Things" 2013 pg-373 to 378

[6] MirzaAbdurRazzaq, Muhammad Ali Qureshi, Sajid Habib Gill, SaleemUllah "Security Issues in the Internet of Things (IoT): A Comprehensive Study" International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017.

[7] A.Arun Raja, R.Naveedha, G.Niranjanadevi and V.Roobini "AN INTERNET OF THINGS (IOT) BASED SECURITY ALERT SYSTEM USING RASPBERRY PI" ASIA PACIFIC INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE Vol. 02 (01) (2016) 37–41

[8] Hafsa Tahir, Ayesha Kanwer and M. Junaid "Internet of Things (IoT): An Overview of Applications and Security Issues Regarding Implementation" INTERNATIONAL JOURNAL

OF MULTIDISCIPLINARY SCIENCES AND ENGINEERING, VOL. 7, NO. 1, JANUARY 2016.

[9] Mario BallanoBarcena and Candid Wueest “Insecurity in the Internet of Things” http:// www.symantec.com Version 1.0 – March 12, 2015.

[10] J. Sathish Kumar and Dhiren R. Patel “A Survey on Internet of Things: Security and Privacy Issues” International Journal of Computer Applications (0975 – 8887) Volume 90 – No 11, March 2014 pg-20 to 26.

[11] Suchitra.C and Vandana C.P “Internet of Things and Security Issues” IJCSMC, Vol. 5, Issue. 1, January 2016, pg.133 – 139.

[12] KANG Kai1, PANG Zhi-bo and WANG Cong “Security and privacy mechanism for health internet of thing” December 2013, 20(Suppl. 2): pg-64–68 www.sciencedirect.com/science/journal/10058885.

[13] Kai Zhao and Lina Ge “Survey on the Internet of Things Security” 2013 Ninth International Conference on Computational Intelligence and Security. pg-663 to 667.